THE MOST TRUSTED SOURCE FOR INFORMATION SECURITY TRAINING, CERTIFICATION, AND RESEARCH

SANS Sydney 2016

3-19 November

HANDS-ON, IMMERSION-STYLE

INFORMATION SECURITY TRAINING

TAUGHT BY REAL-WORLD PRACTITIONERS

Protect your organisation and advance your career with information security training from SANS

SAVE $350 USD

for any 5-6 day course paid for by September 21st

10 courses on

CYBER DEFENSE

PEN TESTING

DIGITAL FORENSICS

SECURITY MANAGEMENT

GIAC-Approved Training

"In-depth, cutting-edge, real-world knowledge provided!"

-James Baker, Pass Key

REGISTER AT

www.sans.org/sydney-2016

SEC301
Intro to Information Security

Hands-On | Mon, 7 Nov - Fri, 11 Nov | Laptop Required | GIAC Cert: GISF | My-Ngoc Nguyen

To determine if the SEC301 course is right for you, ask yourself five simple questions:

- Are you new to information security and in need of an introduction to the fundamentals?
- Are you bombarded with complex technical security terms that you don't understand?
- Are you a non-IT security manager who lays awake at night worrying that your company will be the next mega-breach headline story on the 6 o'clock news?
- Do you need to be conversant in basic security concepts, principles, and terms, even if you don't need "deep in the weeds" detail?
- Have you decided to make a career change to take advantage of the job opportunities in information security and need formal training/certification?

If you answer yes to any of these questions, the **SEC301: Introduction to Information Security** training course is for you. Jump-start your security knowledge by receiving insight and instruction from real-world security experts on critical introductory topics that are fundamental to information security. This completely revised five-day comprehensive course covers everything from core terminology to the basics of computer networks, security policies, incident response, passwords, and even an introduction to cryptographic principles.

This course is designed for students who have no prior knowledge of security and limited knowledge of technology. The hands-on, step-by-step teaching approach will enable you to grasp all of the information presented even if some of the topics are new to you. You'll learn the fundamentals of information security that will serve as the foundation of your InfoSec skills and knowledge for years to come.

www.giac.org/gisf

SEC401
Security Essentials Bootcamp Style

Hands-On | Mon, 7 Nov - Sat, 12 Nov | Laptop Required | GIAC Cert: GSEC | Dr. Eric Cole

Learn the most effective steps to prevent attacks and detect adversaries with actionable techniques that you can directly apply when you get back to work. Learn tips and tricks from the experts so that you can win the battle against the wide range of cyber adversaries that want to harm your environment.

Is **SEC401: Security Essentials Bootcamp Style** the right course for you?

STOP and ask yourself the following questions:

- Do you fully understand why some organisations get compromised and others do not?
- If there were compromised systems on your network, are you confident that you would be able to find them?
- Do you know the effectiveness of each security device and are you certain that they are all configured correctly?
- Are proper security metrics set up and communicated to your executives to drive security decisions?

If you do not know the answers to these questions, SEC401 will provide the information security training you need in a bootcamp-style format that is reinforced with hands-on labs.

PREVENTION IS IDEAL BUT DETECTION IS A MUST

www.giac.org/gsec

SEC504
Hacker Tools, Techniques, Exploits, and Incident Handling

Hands-On | Mon, 7 Nov - Sat, 12 Nov | Laptop Required | GIAC Cert: GCIH | Christopher Crowley

The Internet is full of powerful hacking tools and bad guys using them extensively. If your organisation has an Internet connection or one or two disgruntled employees (and whose doesn't!), your computer systems will get attacked. From the five, ten, or even one hundred daily probes against your Internet infrastructure to the malicious insider slowly creeping through your most vital information assets, attackers are targeting your systems with increasing viciousness and stealth. As defenders, it is essential we understand these hacking tools and techniques.

By helping you understand attackers' tactics and strategies in detail, giving you hands-on experience in finding vulnerabilities and discovering intrusions, and equipping you with a comprehensive incident handling plan, this course helps you turn the tables on computer attackers. It addresses the latest cutting-edge insidious attack vectors, the "oldie-but-goodie" attacks that are still prevalent, and everything in between. Instead of merely teaching a few hack attack tricks, this course provides a time-tested, step-by-step process for responding to computer incidents, and a detailed description of how attackers undermine systems so you can prepare, detect, and respond to them. In addition, the course explores the legal issues associated with responding to computer attacks, including employee monitoring, working with law enforcement, and handling evidence. Finally, students will participate in a hands-on workshop that focuses on scanning for, exploiting, and defending systems. It will enable you to discover the holes in your system before the bad guys do!

www.giac.org/gcih

SEC511
Continuous Monitoring and Security Operations

Hands-On | Mon, 14 Nov - Sat, 19 Nov | Laptop Required | GIAC Cert: GMON | Bryan Simon

We continue to underestimate the tenacity of our adversaries! Organisations are investing a significant amount of time and financial and human resources trying to combat cyber threats and prevent cyber attacks, but despite this tremendous effort organisations are still getting compromised. The traditional perimeter-focused, prevention-dominant approach to security architecture has failed to prevent intrusions. No network is impenetrable, a reality that business executives and security professionals alike have to accept. Prevention is crucial, and we can't lose sight of it as the primary goal. However, a new proactive approach to security is needed to enhance the capabilities of organisations to detect threats that will inevitably slip through their defenses. **SEC511: Continuous Monitoring and Security Operations** will teach you how to strengthen your skills to undertake that proactive approach.

The Defensible Security Architecture, Network Security Monitoring (NSM)/Continuous Diagnostics and Mitigation (CDM)/Continuous Security Monitoring (CSM) taught in this course will best position your organisation or Security Operations Center (SOC) to analyze threats and detect anomalies that could indicate cybercriminal behavior. The payoff for this new proactive approach would be early detection of an intrusion, or successfully thwarting the efforts of attackers altogether.

www.giac.org/gmon

SEC542
Web App Penetration Testing and Ethical Hacking

Hands-On | Mon, 14 Nov - Sat, 19 Nov | Laptop Required | GIAC Cert: GWAPT | Pieter Danhieux

Web applications play a vital role in every modern organisation. But, if your organisation does not properly test and secure its web apps, adversaries can compromise these applications, damage business functionality, and steal data. Unfortunately, many organisations operate under the mistaken impression that a web application security scanner will reliably discover flaws in their systems. ***SEC542 helps students move beyond push-button scanning to professional, thorough, high-value web application penetration testing.***

Customers expect web applications to provide significant functionality and data access. Even beyond the importance of customer-facing web applications, internal web applications increasingly represent the most commonly used business tools within any organisation. Unfortunately, there is no "patch Tuesday" for custom web applications, so major industry studies find that web application flaws play a major role in significant breaches and intrusions. Adversaries increasingly focus on these high-value targets either by directly abusing public-facing applications or by focusing on web apps as targets after an initial break-in. Modern cyber defense requires a realistic and thorough understanding of web application security issues. Anyone can learn to sling a few web hacks, but effective web application penetration testing requires something deeper. ***SEC542 enables students to assess a web application's security posture and convincingly demonstrate the impact of inadequate security that plagues most organisations.***

www.giac.org/gwapt

SEC760
Advanced Exploit Development for Penetration Testers

Hands-On | Mon, 14 Nov - Sat, 19 Nov | Laptop Required | Jake Williams

Vulnerabilities in modern operating systems such as Microsoft Windows 7/8, Server 2012, and the latest Linux distributions are often very complex and subtle. Yet, when exploited by very skilled attackers, these vulnerabilities can undermine an organisation's defenses and expose it to significant damage. Few security professionals have the skillset to discover, let alone even understand at a fundamental level, why the vulnerability exists and how to write an exploit to compromise it. Conversely, attackers must maintain this skillset regardless of the increased complexity. SEC760: Advanced Exploit Development for Penetration Testers teaches the skills required to reverse-engineer 32-bit and 64-bit applications, perform remote user application and kernel debugging, analyze patches for 1-day exploits, and write complex exploit, such as use-after-free attacks against modern software and operating systems.

You Will Learn:

- How to write modern exploits against the Windows 7/8/10 operating systems
- How to perform complex attacks such as use-after-free, kernel exploit techniques, one-day exploitation through patch analysis, and other advanced topics
- The importance of utilizing a Security Development Lifecycle (SDL) or Secure SDLC, along with Threat Modeling
- How to effectively utilize various debuggers and plug-ins to improve vulnerability research and speed
- How to deal with modern exploit mitigation controls aimed at thwarting success and defeating determination

FOR408
Windows Forensic Analysis

Hands-On | Mon, 14 Nov - Sat, 19 Nov | Laptop Required | GIAC Cert: GCFE | Rob Lee, Nick Klein

Every organisation must prepare for cyber-crime occurring on their computer systems and within their networks. Demand has never been higher for analysts who can investigate crimes like fraud, insider threats, industrial espionage, employee misuse, and computer intrusions. Government agencies increasingly require trained media exploitation specialists to recover key intelligence from Windows systems. To help solve these cases, SANS is training a new cadre of the world's best digital forensic professionals, incident responders, and media exploitation masters capable of piecing together what happened on computer systems second by second.

FOR408: Windows Forensic Analysis focuses on building in-depth digital forensics knowledge of the Microsoft Windows operating systems. You can't protect what you don't know about, and understanding forensic capabilities and artifacts is a core component of information security. Learn to recover, analyze, and authenticate forensic data on Windows systems. Understand how to track detailed user activity on your network and how to organize findings for use in incident response, internal investigations, and civil/criminal litigation. Use your new skills for validating security tools, enhancing vulnerability assessments, identifying insider threats, tracking hackers, and improving security policies. Whether you know it or not, Windows is silently recording an unimaginable amount of data about you and your users. FOR408 teaches you how to mine this mountain of data.

www.giac.org/gcfe

FOR578
Cyber Threat Intelligence

Hands-On | Mon, 7 Nov - Fri, 11 Nov | Laptop Required | Robert M. Lee

Make no mistake: current computer network defense and incident response contain a strong element of intelligence and counterintelligence that analysts must understand and leverage in order to defend their computers, networks, and proprietary data.

The collection, classification, and exploitation of knowledge about adversaries – collectively known as cyber threat intelligence – gives network defenders information superiority that can be used to reduce the adversary's likelihood of success with each subsequent intrusion attempt. Responders need accurate, timely, and detailed information to monitor new and evolving attacks, as well as methods to exploit this information to put in place an improved defensive posture. Threat intelligence thus represents a force multiplier for organisations looking to update their response and detection programs to deal with increasingly sophisticated advanced persistent threats.

FOR578 will help network defenders and incident responders:

- Construct and exploit threat intelligence to detect, respond, and defeat advanced persistent threats (APTs)
- Fully analyze successful and unsuccessful intrusions by advanced attackers
- Piece together intrusion campaigns, threat actors, and nation-state organisations
- Manage, share, and receive intelligence on APT adversary groups
- Generate intelligence from their own data sources and share it accordingly
- Identify, extract, and leverage intelligence from APT intrusions
- Expand upon existing intelligence to build profiles of adversary groups
- Leverage intelligence to better defend against and respond to future intrusions

FOR610

Reverse-Engineering Malware: Malware Analysis Tools and Techniques

Hands-On | Mon, 14 Nov - Sat, 19 Nov | Laptop Required | GIAC Cert: GREM | Hal Pomeranz

This popular course explores malware analysis tools and techniques in depth. FOR610 has helped forensic investigators, incident responders, security engineers, and IT administrators acquire the practical skills to examine malicious programs that target and infect Windows systems. Understanding the capabilities of malware is critical to an organisation's ability to derive threat intelligence, respond to information security incidents, and fortify defenses. This course builds a strong foundation for reverse-engineering malicious software using a variety of system and network monitoring utilities, a disassembler, a debugger, and other tools useful for turning malware inside-out.

You Will Learn How To:

- Build an isolated, controlled laboratory environment for analyzing the code and behavior of malicious programs.
- Uncover and analyze malicious JavaScript and VBScript components of web pages, which are often used by exploit kits for drive-by attacks
- Use a disassembler and a debugger to examine the inner workings of malicious Windows executables
- Utilize practical memory forensics techniques to examine the capabilities of rootkits and other malicious program types
- Recognize and understand common assembly-level patterns in malicious code, such as DLL injection and anti-analysis measures
- Assess the threat associated with malicious documents, such as PDF and Microsoft Office files, in the context of targeted attacks
- Derive Indicators of Compromise from malicious executables to perform incident response triage
- Employ network and system-monitoring tools to examine how malware interacts with the file system, registry, network, and other processes in a Windows environment
- Control relevant aspects of the malicious program's behavior through network traffic interception and code patching to perform effective malware analysis
- Bypass a variety of packers and other defensive mechanisms designed by malware authors to misdirect, confuse, and otherwise slow down the analyst

www.giac.org/grem

MGT535

Incident Response Team Management

Hands-On | Thu, 3 Nov - Fri, 4 Nov | Laptop Required | Christopher Crowley

This course discusses the often-neglected topic of managing an incident response team. Given the frequency and complexity of today's cyber attacks, incident response is a critical function for organisations. Incident response is the last line of defense.

Detecting and efficiently responding to incidents requires strong management processes, and managing an incident response team requires special skills and knowledge. A background in information security management or security engineering is not sufficient for managing incidents. On the other hand, incident responders with strong technical skills do not necessarily become effective incident response managers. Special training is necessary.

You Will Learn

- Fundamentals of incident response
- How to establish requirements
- How to set up operations
- Communications
- How to make operations work
- Legal and regulatory issues
- Communications
- Training, education, and awareness

The course has been updated to address current issues such as advanced persistent threat, incident response in the cloud, and threat intelligence.

SANS Sydney 2016 Instructors

Bios on all the instructors can be found at www.sans.org/event/sydney-2016/instructors

Dr. Eric Cole
Faculty Fellow
@drericcole

Christopher Crowley
Certified Instructor
@CCrowMontance

Pieter Danhieux
Certified Instructor
@PieterDanhieux

Nick Klein
Certified Instructor

Rob Lee
Faculty Fellow
@robtlee & @sansforensics

Robert M. Lee
Certified Instructor
@RobertMLee

My-Ngoc Nguyen
Certified Instructor
@MenopN

Hal Pomeranz
Faculty Fellow
@hal_pomeranz

Bryan Simon
Certified Instructor
@BryanOnSecurity

Jake Williams
Certified Instructor
@MalwareJake

SANS SYDNEY 2016

Hotel Information

Training Campus
Grace Hotel Sydney

77 York Street | Sydney, 2000 AU | Phone: + 61 2 9272 6619
www.sans.org/event/sydney-2016/location

Special Hotel Rates Available

A special discounted rate of $250.00 S/D will be honored based on space availability. Rate includes one breakfast per day. Cut-off date for reservations at the SANS rate is 12 October 2016. To make reservations, please call the hotel at 1-800-682-692 (Toll Free within Australia) or 61-2-9272-6619 and give group code SANS041116 to redeem above rate.

The Grace Hotel has been beautifully restored to its former glory, making it one of Sydney's most prominent historical landmark. Located in the heart of Sydney, this hotel offers warm and personal service with the luxury of a 4 1/2 star hotel, exuding a unique blend of old-world charm with modern comfort to meet the needs of guests today. The hotel is located in the centre of Sydney's CBD, on the corner of King and York streets, and is only minutes away from exciting and bustling hubs such as George Street, Pitt Street Mall, Darling Harbour, Martin Place, Circular Quay, and The Rocks.

SANS Sydney 2016 Registration

Register online at www.sans.org/sydney-2016

Select your course or courses and indicate whether you plan to test for GIAC certification.

If the course is still open, the secure, online registration server will accept your registration. Sold-out courses will be removed from the online registration. Everyone with Internet access must complete the online registration form. We do not take registrations by phone.

Pay Early and Save

	DATE	DISCOUNT	DATE	DISCOUNT
Pay & enter code before	**21-9-16**	**$350.00USD**	**5-10-16**	**$200.00USD**

Some restrictions apply.

SANS Sydney 2016

3-19 November

10 courses offered:

SEC301: **Intro to Information Security**
GIAC Cert: GISF | Instructor: My-Ngoc Nguyen

SEC401: **Security Essentials Bootcamp Style**
GIAC Cert: GSEC | Instructor: Dr. Eric Cole

SEC504: **Hacker Tools, Techniques, Exploits, and Incident Handling**
GIAC Cert: GCIH | Instructor: Christopher Crowley

SEC511: **Continuous Monitoring and Security Operations**
GIAC Cert: GMON | Instructor: Bryan Simon

SEC542: **Web App Penetration Testing and Ethical Hacking**
GIAC Cert: GWAPT | Instructor: Pieter Danhieux

SEC760: **Advanced Exploit Development for Penetration Testers**
Instructor: Jake Williams

FOR408: **Windows Forensic Analysis**
GIAC Cert: GCFE | Instructors: Rob Lee, Nick Klein

FOR578: **Cyber Threat Intelligence**
Instructor: Robert M. Lee

FOR610: **Reverse-Engineering Malware: Malware Analysis Tools and Techniques**
GIAC Cert: GREM | Instructors: Hal Pomeranz

MGT535: **Incident Response Team Management**
Instructor: Christopher Crowley

REGISTER AT
sans.org/sydney-2016

CONTACT INFORMATION

For further information, please contact:
asiapacific@sans.org | 02 6287 7247
0402 067 768 (Steven Armitage) | 0439 911 663 (Gusto Simandjuntak)